МИНИСТЕРСТВО ОБРАЗОВАНИЯ И МОЛОДЁЖНОЙ ПОЛИТИКИ СВЕРДЛОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СВЕРДЛОВСКОЙ ОБЛАСТИ «АСБЕСТОВСКИЙ ПОЛИТЕХНИКУМ»

УТВЕРЖДАЮ
Директор ГАПОУ СО
«Асбестовский политехникум»
_____ В.А. Суслопаров
«29» июня 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.10 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для специальности СПО
09.02.03 «Программирование в компьютерных системах»
Форма обучения – очная
Срок обучения 3 года 10 месяцев

Асбест
2020

Рабочая программа учебной дисциплины «**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**» разработана на основе маркетинговых исследований и пожеланий потенциальных работодателей к результату образования выпускников по специальности **09.02.03 «Программирование в компьютерных системах»** среднего профессионального образования, утверждённого приказом Минобрнауки №804 от 28 июля 2014 года.

Организация-разработчик: ГАПОУ СО «Асбестовский политехникум»

Разработчик:

Савина Ольга Николаевна, преподаватель, высшая квалификационная категория, ГАПОУ СО «Асбестовский политехникум», г. Асбест

РАССМОТРЕНО
цикловой комиссией информационных и экономических дисциплин,
протокол № 6
«23» июня 2020 г.
Председатель _____ Е.А. Ярышева

СОГЛАСОВАНО
Методическим советом, протокол № 3
«25» июня 2020 г.
Председатель _____ Н.Р. Караваева

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа вариативной учебной дисциплины является частью основной профессиональной образовательной программы по специальности СПО 230115 «Программирование в компьютерных системах»

Общие компетенции

ОК 1.Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Профессиональные компетенции:

ПК 2.5 Выполнять установку, настройку антивирусных программ

ПК 2.6 Выполнять сканирование компьютера с помощью антивирусных программ

ПК 2.7 Осуществлять настройку систем шифрования данных

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: блок общепрофессиональных дисциплин (вариативная часть цикла)

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен уметь:

- выявлять вредоносное программное обеспечение на компьютере;
- избавляться от вредоносного ПО средствами антивирусных программ, выбирая их в соответствии с возможностями и особенностями программы;
- применяя различные системы шифрования информации шифровать и дешифровать информацию;
- выполнять установку, настройку антивирусных программ;
- выполнять сканирование компьютера с помощью антивирусных программ;
- осуществлять настройку систем шифрования данных

В результате освоения дисциплины обучающийся должен знать:

- базовые понятия, основные принципы и аспекты информационной безопасности;
- правовые основы защиты информации меры ответственности за нарушение законодательств в информационной сфере;
- характеристики безопасной и надёжной системы, политика безопасности;
- автоматизированные системы обработки данных, элементы АСОД, уязвимость и дестабилизирующие факторы АСОД;
- задачи, методы и функции защиты информации;
- основные термины криптологии, разновидности криптосистем, суть различных алгоритмов шифрования;
- определение угроз, основные угрозы доступности, целостности и конфиденциальности;
- классы антивирусных программ, классификация вирусов, типы вирусов, пути проникновения вируса в ПК.

1.4. Количество часов на освоение учебной дисциплины:

максимальной учебной нагрузки обучающегося 48 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 32 часа;

самостоятельной работы обучающегося 16 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	**48**
Обязательная аудиторная учебная нагрузка (всего)	**32**
в том числе:	
практические занятия	8
Самостоятельная работа обучающегося (всего)	**16**
Промежуточная аттестация в форме ***дифференцированного зачета***	

2.2. Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, практические занятия и самостоятельная работа обучающихся	Количество часов	Уровень освоения
1	2	3	4
Тема 1. Общие проблемы безопасности. Роль и место информационной безопасности.	**Содержание учебного материала**	**4**	
	1. Основные принципы ИБ; национальная безопасность; 2. Защита информации (ЗИ), основные направления ЗИ; правовые основы защиты.	2	*1*
	Самостоятельная работа	2	*3*
	Поиск и анализ дополнительных источников регулирующих нормы права в информационной сфере.		
Тема 2. Предмет и объекты защиты информации в автоматизированных системах обработки данных (АСОД).	**Содержание учебного материала**	**8**	
	1. Надёжность и уязвимость информации в АСОД; 2. Элементы и объекты защиты в АСОД; 3. Дестабилизирующие факторы, причины их возникновения; системы и механизмы ЗИ;	6	*1*
	Самостоятельная работа	**2**	*3*
	Изучение примеров АСОД, методов защиты АСОД.		
Тема 3. Угрозы. Компьютерные вирусы и антивирусные программы.	**Содержание учебного материала**	**14**	
	1. Основные определения и классификация угроз. 2. Наиболее распространенные угрозы доступности, целостности, конфиденциальности. 3. Компьютерный вирус, история, классификация вирусов. 4. Алгоритмы вирусов, признаки возникновения, методы защиты от вирусов. 5. Антивирусные программы, возможности и особенности некоторых антивирусных программ.	10	*1*
	Самостоятельная работа	4	*3*
	Новейшие вирусы, характеристики, новейшие антивирусные программы.		
Тема 4. Защита информации в персональных компьютерах, сетях ЭВМ.	**Содержание учебного материала**	**6**	
	1. Особенности защиты информации в персональных ЭВМ; 2. Архитектура механизмов защиты информации в сетях ЭВМ; защита информации в операционных системах и базах данных.	4	*1*
	Самостоятельная работа	**2**	*3*
	Самостоятельное изучение программы Ad-Aware SE 2007 – средство обеспечения безопасности ПК, элементы интерфейса, технологии которые использует программа для поиска и устранения угроз. Изучение дополнительных программно-технических изделий, предназначенных для защиты информации в ПК.		

Тема 5. Криптографические методы защиты информации.	**Содержание учебного материала**	**16**	
	Криптология. Методы криптографического преобразования: шифрование, кодирование, системы с открытым ключом, электронная цифровая подпись. Криптографические стандарты..	2	*1*
	Практические занятия		
	1. Шифрование заменой (подстановка) – шифр Вижинера; 2. Метод перестановок. 3. Монофоническая замена; 4. Шифрование с помощью аналитических преобразований.	8	*2*
	Самостоятельная работа	**6**	*3*
	История её развития криптологии. Самостоятельное изучение различных методов шифрования, и кодирования.		
	Итого:	**48**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);

2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)

3.– продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Реализация программы учебной дисциплины требует наличия полигона вычислительной техники.

Наименование оборудования, приспособлений, инструментов, оснастки, наглядных пособий и документации определена в соответствии с требованиями к охране труда и техники безопасности на рабочем месте.

Оборудование учебного кабинета:

1. Планшеты
2. Видеопроектор
3. Интерактивна доска
4. Акустическая система

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий:

1. Галатенко В.А. Основы информационной безопасности Интернет-университет информационных технологий - ИНТУИТ.ру, 2008
2. Кирсанов А.П. Теория информационных технологий и систем Интернет-университет информационных технологий - ИНТУИТ.ру, 2009
3. Кодекс Российской Федерации об административных правонарушениях. М.: Инфра-М, 2002. 304 с.
4. Партыка Т.Л., Попов И.И. Информационная безопасноть: учебное пособие для студентов учреждений учреждений СПО: М.ФОРУМ, 2008

Перечень дополнительной литературы:

1. Ложников П.С., Михайлов Е.М. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft Интернет-университет информационных технологий - БИНОМ. Лаборатория знаний, 2008 г., 247 стр.
2. Мельников В.П. Информационная безопасность: Учеб. пособие для студ. СПО. – М.: Издательский центр «Академия», 2009
3. Федеральный закон «Об ин6формации, информатизации и защите информации». Собрание законодательства Российской Федерации. 20 февраля 1995 г. Официальное издание. М.: Издательство «Юридическая литература», Администрация президента Российской федерации. С. 1213-1225.
4. Фороузан Б.А. Концепцияи криптографии и безопасности сети Интернет-университет информационных технологий - ИНТУИТ.ру, Эком, БИНОМ. Лаборатория знаний, 2010 г., 784 стр.

5. Хаулет Т. Защитные средства с открытыми исходными текстами БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий - ИНТУИТ.ру, 2007

Перечень рекомендуемых Интернет-ресурсов:

1. Курс Введение в защиту информации от внутренних ИТ-угроз http://www.intuit.ru/department/security/infowatch/
2. Курс Инструментальные средства обеспечения безопасности http://www.intuit.ru/department/security/issec/
3. Курс Основы информационной безопасности http://www.intuit.ru/department/security/secbasics/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

ГАПОУ СО «Асбестовский политехникум», реализующее подготовку по учебной дисциплине «Информационная безопасность», обеспечивает организацию и проведение промежуточной аттестации и текущего контроля, демонстрируемых студентами знаний, умений и навыков. Текущий контроль проводится преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Формы и методы текущего контроля по учебной дисциплине самостоятельно разрабатываются преподавателем, рассматриваются на заседании цикловой комиссии информационных технологий, согласуются с работодателями, методическим советом и доводятся до сведения обучающихся в начале обучения.

Обучение по учебной дисциплине завершается проведением дифференцированного зачета в форме собеседования по вопросам.

Такая форма аттестации позволяет охватить весь пройденный теоретический материал по дисциплине, проверить системность знаний, а также умение применять полученные знания на практике.

На этапе промежуточной аттестации по медиане качественных оценок индивидуальных образовательных достижений преподавателем определяется интегральная оценка освоенных обучающимис профессиональных и общих компетенций как результатов освоения учебной дисциплины.

Для текущего контроля преподавателем создаются фонды оценочных средств (ФОС).

Результаты обучения (освоенные умения, усвоенные знания)	Показатели освоения результата	Формы и методы контроля и оценки результатов обучения
Усвоенные знания: • базовые понятия, основные принципы и аспекты информационной безопасности; • правовые основы защиты информации и меры ответственности за нарушение законодательства в информационной сфере; • характеристики безопасной и надёжной систем, политика безопасности; • автоматизированные системы обработки данных, элементы объекты АСОД, уязвимость и дестабилизирующие факторы АСОД; • задачи, методы и функции защиты информации; • основные термины криптологии, разновидности криптосистем, суть различных алгоритмов шифрования; • определение угрозы, основные угрозы доступности, целостности и конфиденциальности. • классы антивирусных программ, классификация вирусов, типы вирусов, пути проникновения вируса в ПК.	Правильно и корректно отвечает на поставленные вопросы по базовым понятиям информационной защиты	• фронтальный опрос • письменный опрос (по контрольным вопросам, тестам) • собеседование
Освоенные умения: • выявлять вредоносное программное обеспечение на компьютере; • избавляться от вредоносного ПО средствами антивирусных программ, выбирая их в соответствии с возможностями и особенностями программы; • применяя различные системы шифрования информации шифровать и дешифровать информацию. • выполнять установку, настройку антивирусных программ; • выполнять сканирование компьютера с помощью антивирусных программ • осуществлять настройку систем шифрования данных	• Устанавливает антивирусные программы • Использует различные методы шифрования (дешифрования) информации	проверка результата выполнения практической работы